

# IEEE Std 3006.5™-2014

Recommended Practice for the  
Use of Probability Methods for  
Conducting a Reliability Analysis of  
Industrial and Commercial Power  
Systems





# **IEEE Recommended Practice for the Use of Probability Methods for Conducting a Reliability Analysis of Industrial and Commercial Power Systems**

Sponsor

**Technical Books Coordinating Committee  
of the  
IEEE Industry Applications Society**

Approved 10 December 2014

**IEEE-SA Standards Board**

**Abstract:** Described in this recommended practice are ways for using probability methods to conduct a reliability analysis of industrial and commercial power systems. It is likely to be of greatest value to the power-oriented engineer with limited experience in the area of reliability. It can also be an aid to all engineers responsible for the electrical design of industrial and commercial power systems.

**Keywords:** availability, common cause failure, IEEE 3006.5™, reliability, reliability analysis, time to failure data

---

The Institute of Electrical and Electronics Engineers, Inc.  
3 Park Avenue, New York, NY 10016-5997, USA

Copyright © 2015 by The Institute of Electrical and Electronics Engineers, Inc.  
All rights reserved. Published 17 February 2015. Printed in the United States of America.

IEEE is a registered trademark in the U.S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated.

PDF: ISBN 978-0-7381-9471-4 STD20067  
Print: ISBN 978-0-7381-9472-1 STDPD20067

*IEEE prohibits discrimination, harassment, and bullying.*

For more information, visit [http://www.ieee.org/web/aboutus/what\\_is/policies/p9-26.html](http://www.ieee.org/web/aboutus/what_is/policies/p9-26.html).

*No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.*

## **Important Notices and Disclaimers Concerning IEEE Standards Documents**

IEEE documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page, appear in all standards and may be found under the heading “Important Notice” or “Important Notices and Disclaimers Concerning IEEE Standards Documents.”

### **Notice and Disclaimer of Liability Concerning the Use of IEEE Standards Documents**

IEEE Standards documents (standards, recommended practices, and guides), both full-use and trial-use, are developed within IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (“IEEE-SA”) Standards Board. IEEE (“the Institute”) develops its standards through a consensus development process, approved by the American National Standards Institute (“ANSI”), which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and participate without compensation from IEEE. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

IEEE does not warrant or represent the accuracy or content of the material contained in its standards, and expressly disclaims all warranties (express, implied and statutory) not included in this or any other document relating to the standard, including, but not limited to, the warranties of: merchantability; fitness for a particular purpose; non-infringement; and quality, accuracy, effectiveness, currency, or completeness of material. In addition, IEEE disclaims any and all conditions relating to: results; and workmanlike effort. IEEE standards documents are supplied “AS IS” and “WITH ALL FAULTS.”

Use of an IEEE standard is wholly voluntary. The existence of an IEEE standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard.

In publishing and making its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document, should rely upon his or her own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

IN NO EVENT SHALL IEEE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE PUBLICATION, USE OF, OR RELIANCE UPON ANY STANDARD, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

### **Translations**

The IEEE consensus development process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English version published by IEEE should be considered the approved IEEE standard.

## Official statements

A statement, written or oral, that is not processed in accordance with the IEEE-SA Standards Board Operations Manual shall not be considered or inferred to be the official position of IEEE or any of its committees and shall not be considered to be, or be relied upon as, a formal position of IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position of IEEE.

## Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE. However, IEEE does not provide consulting information or advice pertaining to IEEE Standards documents. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important that any responses to comments and questions also receive the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to comments or questions except in those cases where the matter has previously been addressed. For the same reason, IEEE does not respond to interpretation requests. Any person who would like to participate in revisions to an IEEE standard is welcome to join the relevant IEEE working group.

Comments on standards should be submitted to the following address:

Secretary, IEEE-SA Standards Board  
445 Hoes Lane  
Piscataway, NJ 08854 USA

## Laws and regulations

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document does not imply compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

## Copyrights

IEEE draft and approved standards are copyrighted by IEEE under U.S. and international copyright laws. They are made available by IEEE and are adopted for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making these documents available for use and adoption by public authorities and private users, IEEE does not waive any rights in copyright to the documents.

## Photocopies

Subject to payment of the appropriate fee, IEEE will grant users a limited, non-exclusive license to photocopy portions of any individual standard for company or organizational internal use or individual, non-commercial use only. To arrange for payment of licensing fees, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

## Updating of IEEE Standards documents

Users of IEEE Standards documents should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect.

Every IEEE standard is subjected to review at least every ten years. When a document is more than ten years old and has not undergone a revision process, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE standard.

In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit the IEEE-SA Website at <http://ieeexplore.ieee.org/xpl/standards.jsp> or contact IEEE at the address listed previously. For more information about the IEEE-SA or IEEE's standards development process, visit the IEEE-SA Website at <http://standards.ieee.org>.

## Errata

Errata, if any, for all IEEE standards can be accessed on the IEEE-SA Website at the following URL: <http://standards.ieee.org/findstds/errata/index.html>. Users are encouraged to check this URL for errata periodically.

## Patents

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE-SA Website at <http://standards.ieee.org/about/sasb/patcom/patents.html>. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

Essential Patent Claims may exist for which a Letter of Assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

## Participants

At the time this IEEE recommended practice was completed, the Power System Reliability Working Group had the following membership:

### **Robert Arno, *Chair***

Michael Anthony  
Timothy Coyle

Neal Dowling  
Masoud Pourali  
Robert Schuerger

Michael Simon  
Joseph Weber

At the time this IEEE recommended practice was submitted by the Power System Reliability Working Group to the IEEE-SA Standards Board for approval, the 3006.5 Working Group had the following membership:

### **Masoud Pourali, *Chair***

Michael Anthony  
Timothy Coyle

Neal Dowling  
Robert Schuerger

Michael Simon  
Joseph Weber

The following members of the individual balloting committee voted on this recommended practice. Balloters may have voted for approval, disapproval, or abstention.

William Ackerman  
William Braun  
Frederick Brockhurst  
Chris Brooks  
Bill Brown  
William Byrd  
Paul Cardinal  
Sean Carr  
Daniel Conte  
Carey Cook  
Brian Cramer  
Alireza Daneshpooy  
Ray Davis  
Douglas Dorr  
Randall Dotson  
Neal Dowling  
Timothy Gauthier  
Randall Groves  
Song Jin  
Laszlo Kadar

John Kay  
Yuri Khersonsky  
Jim Kulchisky  
Saumen Kundu  
Ed Larsen  
Michael Lauxman  
Wei-Jen Lee  
Edward McCall  
T. David Mills  
Sujeet Mishra  
Daleep Mohla  
Edrin Murzaku  
Daniel Neeser  
Dennis Neitzel  
Gearold O. H. Eidhin  
Lorraine Padden  
Mirko Palazzo  
Louie Powell  
Iulian Profir  
Annette Reilly  
Kenneth Rempe

Michael Roberts  
Charles Rogers  
Daniel Sabin  
Bartien Sayogo  
Ted Schoenberg  
Robert Schuerger  
Robert Seitz  
Michael Simon  
David Singleton  
Jerry Smith  
John Spare  
March Stutzman  
Michael Swearingen  
David Tepen  
Marcelo Valdes  
Peter Walsh  
Yingli Wen  
Kenneth White  
Jian Yu  
Shuhui Zhang



When the IEEE-SA Standards Board approved this recommended practice on 10 December 2014, it had the following membership:

**John Kulick**, *Chair*  
**Jon Walter Rosdahl**, *Vice Chair*  
**Richard H. Hulett**, *Past Chair*  
**Konstantinos Karachalios**, *Secretary*

Peter Balma  
Farooq Bari  
Ted Burse  
Clint Chaplin  
Stephen Dukes  
Jean-Philippe Faure  
Gary Hoffman

Michael Janezic  
Jeffrey Katz  
Joseph L. Koepfinger\*  
David J. Law  
Hung Ling  
Oleg Logvinov  
T. W. Olsen  
Glenn Parsons

Ron Petersen  
Adrian Stephens  
Peter Sutherland  
Yatin Trivedi  
Phil Winston  
Don Wright  
Yu Yuan

\*Member Emeritus

Also included are the following nonvoting IEEE-SA Standards Board liaisons:

Richard DeBlasio, *DOE Representative*  
Michael Janezic, *NIST Representative*

Julie Alessi  
*IEEE-SA Content Production and Management*

Lisa Perry  
*IEEE-SA Technical Program Operations*

## Introduction

This introduction is not part of IEEE Std 3006.5™-2014, IEEE Recommended Practice for the Use of Probability Methods for Conducting a Reliability Analysis of Industrial and Commercial Power Systems.
--

### IEEE 3000 Standards Collection®

This recommended practice was developed by the Technical Books Coordinating Committee of the Industrial and Commercial Power Systems Department of the Industry Applications Society as part of a project to repackage the popular IEEE Color Books®. The goal of this project is to speed up the revision process, eliminate duplicate material, and facilitate use of modern publishing and distribution technologies.

When this project is completed, the technical material in the thirteen IEEE Color Books will be included in a series of new standards—the most significant of which will be a new standard, IEEE Std 3000™, Recommended Practice for the Engineering of Industrial and Commercial Power Systems. The new standard will cover the fundamentals of planning, design, analysis, construction, installation, startup, operation, and maintenance of electrical systems in industrial and commercial facilities. Approximately 60 additional dot standards, organized into the following categories, will provide in-depth treatment of many of the topics introduced by IEEE Std 3000™:

- Power Systems Design (3001 series)
- Power Systems Analysis (3002 series)
- Power Systems Grounding and Bonding (3003 series)
- Protection and Coordination (3004 series)
- Emergency, Standby Power, and Energy Management Systems (3005 series)
- Power Systems Reliability (3006 series)
- Power Systems Maintenance, Operations, and Safety (3007 series)

In many cases, the material in a dot standard comes from a particular chapter of a particular IEEE Color Book. In other cases, material from several IEEE Color Books has been combined into a new dot standard.

The material in this recommended practice largely comes from Chapter 2 of IEEE Std 493™ (*IEEE Gold Book*).

### IEEE Std 3006.5™

This recommended practice provides the theoretical background to perform basic reliability analysis. Some basic concepts of probability theory are discussed, as these are essential to the understanding and development of quantitative reliability. The objective of this recommended practice is to provide the basic theoretical background for the reliability analysis used in the planning and design of industrial and commercial electric power distribution systems.

The design of reliable industrial and commercial power distribution systems is important because of the high cost associated with power outages. It is necessary to consider the cost of power outages when making design decisions for new and existing power distribution systems as well as to have the ability to make quantitative cost-versus-reliability trade-off studies. This recommended practice may be considered as a prerequisite to all other Power Systems Reliability dot standards (3006 series).

## Contents

1. Overview .....	1
1.1 Scope .....	1
2. Normative references.....	1
3. Definitions, acronyms, and abbreviations .....	2
3.1 Definitions .....	2
3.2 Acronyms and abbreviations .....	4
4. Calculation reference.....	5
4.1 Summary.....	5
5. Review of basic probability.....	8
5.1 Sample space .....	8
5.2 Event.....	8
5.3 Combinatorial properties of event probabilities .....	8
5.4 Reliability and availability.....	10
5.5 Time to failure data.....	13
6. Defining frequency and duration of outages and interruptions, $\lambda$ , <i>MTBF</i> .....	13
6.1 Frequency of failures, outages .....	14
6.2 Duration of outages and interruptions .....	14
7. Probability distributions .....	14
7.1 Probability density functions .....	14
7.2 Cumulative distribution function.....	14
7.3 Hazard function .....	15
7.4 Exponential distribution.....	15
7.5 Weibull distribution.....	16
7.6 Calculating reliability for the exponential distribution .....	17
8. Methods of reliability and availability analysis.....	21
8.1 Qualitative system analysis.....	21
8.2 Numerical methods.....	31
9. Performing reliability and availability analyses .....	33
9.1 Modeling limitations.....	34
9.2 Modeling solutions .....	34
10. Common cause failures (CCF) .....	34
10.1 Common cause failure analysis procedure .....	35
Annex A (informative) Bibliography .....	36



# IEEE Recommended Practice for the Use of Probability Methods for Conducting a Reliability Analysis of Industrial and Commercial Power Systems

*IMPORTANT NOTICE: IEEE Standards documents are not intended to ensure safety, security, health, or environmental protection, or ensure against interference with or from other devices or networks. Implementers of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, and interference protection practices and all applicable laws and regulations.*

*This IEEE document is made available for use subject to important notices and legal disclaimers. These notices and disclaimers appear in all publications containing this document and may be found under the heading “Important Notice” or “Important Notices and Disclaimers Concerning IEEE Documents.” They can also be obtained on request from IEEE or viewed at <http://standards.ieee.org/IPR/disclaimers.html>.*

## 1. Overview

### 1.1 Scope

This recommended practice describes how to use probability methods for conducting a reliability analysis of industrial and commercial power systems. It is likely to be of greatest value to the power-oriented engineer with limited experience in the area of reliability. It can also be an aid to all engineers responsible for the electrical design of industrial and commercial power systems.

## 2. Normative references

The following referenced documents are indispensable for the application of this document (i.e., they must be understood and used, so each referenced document is cited in text and its relationship to this document is explained). For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

IEEE Std 493™-2007, Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems (*IEEE Gold Book™*).<sup>1,2</sup>

### 3. Definitions, acronyms, and abbreviations

#### 3.1 Definitions

For the purposes of this document, the following terms and definitions apply. The *IEEE Standards Dictionary Online* should be consulted for terms not defined in this clause.<sup>3</sup>

Some commonly used terms in system reliability analyses are defined here; these terms are also used in the wider context of system reliability activities. These definitions are referenced in several reliability publications and the formulas can be verified in the Reliability Analysis Center's Reliability Toolkit: Commercial Practices Edition, page 12 [B15], or MIL-STD-339 [B7].<sup>4</sup>

**availability:** (A) (general) The ability of an item—under combined aspects of its reliability, maintainability, and maintenance support—to perform its required function at a stated instant of time or over a stated period of time. (B) (as a performance metric for individual components or a system) The long-term average fraction of time that a component or system is in service and satisfactorily performing its intended function. (C) (as a future prediction) The instantaneous probability that a component or system will be in operation at time  $t$ .

**common cause failure:** Common cause failures are dependent events in which a single failure or condition affects the operation of two or more devices that would otherwise be considered independent.

**component:** A piece of electrical or mechanical equipment viewed as an entity for the purpose of reliability evaluation.

**cumulative distribution function (CDF):** In statistics, the mathematical equation that sums the results of a distribution function over time (e.g., total failures in five years) or possible results (e.g., probability of rolling a 7 or lower with two dice). The cumulative distribution function of  $T$ ,  $F(t) = \Pr(T \leq t)$ , gives the probability that a unit will fail before time  $t$  [B11].

**distribution functions:** In statistics, the mathematical equation that relates one variable to another variable such as time (e.g., failures/year) or possible results (e.g., probability of rolling a specific number with two dice).

**failure (f):** The termination of the ability of a component or system to perform a required function.

**failure mode:** The manner of failure. Failure mode is a description of how we can observe a fault.

**failure rate ( $\lambda$ ):** The mean (arithmetic average) number of failures of a component and/or system per unit exposure time. The most common unit in reliability analyses is hours (h) or years (y). Therefore, the failure rate is expressed in failures per hour (f/h) or failures per year (f/y). *Syn:* **forced outage rate**.

---

<sup>1</sup> The IEEE standards or products referred to in this clause are trademarks of The Institute of Electrical and Electronics Engineers, Inc.

<sup>2</sup> IEEE publications are available from The Institute of Electrical and Electronics Engineers, 445 Hoes Lane, Piscataway, NJ 08854, USA (<http://standards.ieee.org/>).

<sup>3</sup> *IEEE Standards Dictionary Online* subscription is available at:  
[http://www.ieee.org/portal/innovate/products/standard/standards\\_dictionary.html](http://www.ieee.org/portal/innovate/products/standard/standards_dictionary.html).

<sup>4</sup> The numbers in brackets correspond to those of the bibliography in Annex A.

**inherent availability (Ai):** Long-term average fraction of time that a component or system is in service and satisfactorily performing its intended function. Ai considers only downtime for repair of failures. No logistics time, preventive maintenance, etc., is included.

**log-normal distribution:** A continuous distribution in which the logarithm of a variable has a normal distribution.

**maintenance downtime (Mdt):** The total downtime for scheduled maintenance (including logistics time, spare parts availability, crew availability, etc.) for a given time period (Tp) (hours).

**mean downtime (MDT):** The average downtime caused by scheduled and unscheduled maintenance, including any logistics time. *Syn:* **mean time to restore system (MTTRS).**

**mean time between failures (MTBF):** MTBF is the arithmetic mean of the times (observed or calculated) between random failures of a component or system.

**mean time between maintenance (MTBM):** The average time between all maintenance events, scheduled and unscheduled, and includes any associated logistics time.

**mean time to failure (MTTF):** The mean exposure time between consecutive repairs (or installations) of a component and the next failure of that component. MTTF is commonly found for non-repairable items such as bulbs.

**mean time to maintain (MTTM):** The average time it takes to maintain a component, including logistics time. MTTM is primarily a measure of the preventive maintenance frequency and durations.

**mean time to repair (MTTR or simply r):** The mean time to replace or repair a failed component. Logistics time associated with the repair, such as parts acquisitions, crew mobilization, are not included. It can be estimated by dividing the summation of repair times by the number of repairs and, therefore, is practically the average repair time. The most common unit in reliability analyses is hours (h/f).

**Monte Carlo simulation:** The use of computer program using probability algorithms to perform repeated analysis of random variables in order to determine numerical values of reliability metrics.

**operational availability (Ao):** Long-term average fraction of time that a component or system is in service and satisfactorily performing its intended function. Ao differs from Ai in that it includes all downtime. Included are downtime for the repair of failures, scheduled maintenance, and any logistics time required (such as obtaining the necessary parts and scheduling the technician to perform the repair).

**probability density function (PDF):** The probability density function for a continuous random variable T is the derivative of cumulative distribution function (F(t)) with respect to t. The PDF can be used to represent relative frequency of failure times as a function of time [B9].

**random variable (r.v.):** A random variable is a variable whose possible values are numerical outcomes of a random phenomenon. Random variables can be divided into two classes: discrete and continuous.

**reliability:** The probability that a component or system will perform required functions under stated conditions for a stated period of time t, or (for discrete missions) a stated number of demands.

**repair downtime (Rdt):** The total downtime for unscheduled maintenance (excluding logistics time) for a given total period (hours).

**repair logistics time (Rlt):** The total logistics time for unscheduled maintenance for a given total period (hours).

**system:** A group of components connected or associated in a fixed configuration to perform a specified function.

**total downtime events (Tde):** The total number of downtime events (including scheduled maintenance and failures) during the total period (previously referred to as all actions, maintenance, and repair).

**total failures (Tf):** The total number failures during the total period.

**total maintenance actions (Tma):** The total number of scheduled maintenance actions during the total period.

**total period (Tp):** The calendar time over which data for the item was collected (hours).

**year (y):** The unit of time measurement approximately equal to 8765.81277 hours (h). Any rounding of this value will have adverse effects on analyses depending on the magnitude of that rounding; 8766 is used commonly as it is the result of rounding to  $365.25 \times 24$  (which accounts for a leap year every 4th year); 8760, which is  $365 \times 24$ , is the most commonly used value in power reliability field. By convention, 8760 will be used throughout this recommended practice.

## 3.2 Acronyms and abbreviations

Ai	inherent availability
Ao	operational availability
ATS	automatic transfer switch
BBN	Bayesian belief network
BN	Bayesian network
CDF	cumulative distribution function
CCF	common cause failure
FMEA	failure mode and effects analysis
Mdt	maintenance downtime
MDT	mean downtime
m-g	motor-generator
MTBF	mean time between failures
MTBM	mean time between maintenance
MTTF	mean time to failure
MTTR	mean time to repair
O&M	operations and maintenance
PDF	probability density function
PDU	power distribution unit
RBD	reliability block diagram
RCM	reliability centered maintenance
Rdt	repair downtime



Rlt	repair logistics time
SPOF	single point of failure
Tde	total downtime events
Tf	total failures
Tma	total maintenance actions
Tp	total period

## 4. Calculation reference

### 4.1 Summary

A summary of the definitions is compiled in Table 1. This table provides a quick reference for some of the formulas used and defined later in this document.

**Table 1—Definition summary**

Calculated data	Formula for calculation
Ai, inherent availability	$A_i = \text{MTBF} / (\text{MTBF} + \text{MTTR})$
Ao, operational availability	$A_o = \text{MTBM} / (\text{MTBM} + \text{MDT})$
$\lambda$ , failure rate (f/h)	$\lambda = T_f / T_p$
$\lambda$ , failure rate (f/y)	$\lambda = T_f / (T_p / 8760)$
MDT, mean downtime (h)	$\text{MDT} = (\text{Rdt} + \text{Rlt} + \text{Mdt}) / T_{de}$
MTBF, mean time between failures (h)	$\text{MTBF} = T_p / T_f$
MTBM, mean time between maintenance (h)	$\text{MTBM} = T_p / T_{de}$
MTTM, mean time to maintain (h)	$\text{MTTM} = \text{Mdt} / T_{ma}$
MTTR, mean time to repair (h)	$\text{MTTR} = r = \text{Rdt} / T_f$
R(t), reliability	$R(t) = e^{-\lambda t}$
Downtime hours per year (DHY)	$\text{DHY} = (1 - A_o) \times 8760$
$\lambda_r$ , downtime hours per year (DHY)	$\text{DHY} = \lambda_r$ , where $\lambda$ is the failure rate per year

**Example 1.** Part of a life cycle of a single repairable component is shown in Figure 1, and a legend describing the variables is shown in Table 2. Table 3 presents the recorded time for each period during the data collection time. Calculate all indices defined in Table 1.

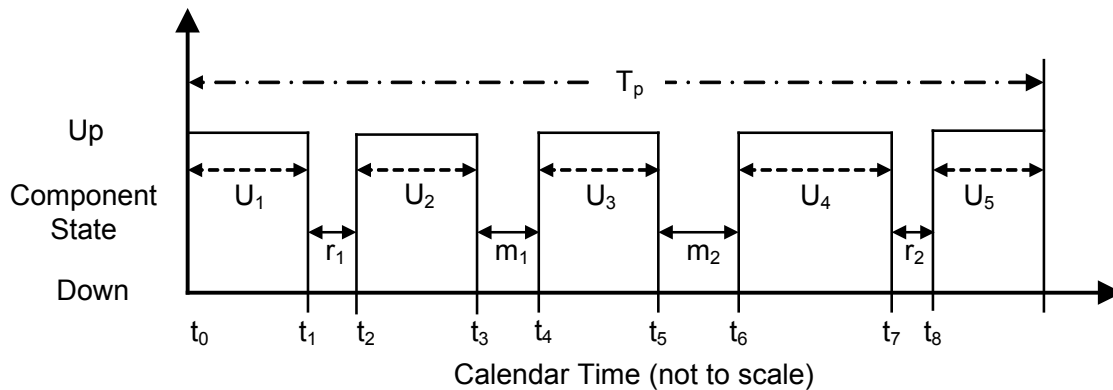


Figure 1—Cyclic operation of a component during the period of data collection

Table 2—Variables legend

Variable	Description
$T_p$	Total period—Calendar time over which the data for the component was collected expressed in hours
$U_i$	$i^{\text{th}}$ operational or up time for a component
$r_i$	$i^{\text{th}}$ repair or restoration time for an unscheduled component-forced outage (i.e., duration of an unscheduled maintenance event) expressed in hours
$m_i$	$i^{\text{th}}$ duration of a scheduled maintenance event expressed in hours
$t_i$	Calendar time when the transition between a component's up or operating state and down state occurs

Table 3—Recorded time for each period during the data collection time

Calendar time	Magnitude of $t_i$ (calendar hours)	Variable	Magnitude of variable (hours)
$t_0 - t_1$ ( $t_0$ through $t_1$ )	1000	$U_1$	1000
$t_1 - t_2$	1010	$r_1$	10
$t_2 - t_3$	2010	$U_2$	1000
$t_3 - t_4$	2110	$m_1$	100
$t_4 - t_5$	2610	$U_3$	500
$t_5 - t_6$	2810	$m_2$	200
$t_6 - t_7$	4060	$U_4$	1250
$t_7 - t_8$	4100	$r_2$	40
$t_8 - T_p$	5000	$U_5$	900

**Solution:** What follows are presentations of the calculations of various indices discussed in 3.1:

1. Total component data collection period –  $T_p = 5000$  hours
2. Total component repair or restoration time (i.e., down time) due to component-forced outages (i.e., unscheduled maintenance)

$$Rdt = r_1 + r_2 = 10 + 40 = 50 \text{ hours}$$

3. Total component scheduled maintenance down time

$$Mdt = m_1 + m_2 = 100 + 200 = 300 \text{ hours}$$

4. Total component operating (uptime)

$$T_{\text{Uptime}} = U_1 + U_2 + U_3 + U_4 + U_5 = 1000 + 1000 + 500 + 1250 + 900 = 4650 \text{ hours}$$

5. Total number of forced component outages –  $T_f = 2$
6. Total number of component scheduled maintenance outages –  $T_{ma} = 2$

7. Mean time to repair (MTTR)

$$MTTR = Rdt / T_f = 50 / 2 = 25 \text{ hours}$$

8. Mean time to maintain (MTTM)

$$MTTM = Mdt / T_{ma} = 300 / 2 = 150 \text{ hours}$$

9. Mean down time (MDT)

$$MDT = (Rdt + Rlt + Mdt) / (T_f + T_{ma}) = (50 + 300) / (2 + 2) = 87.5 \text{ hours}$$

10. Mean up time (MUT)

$$MUT = \frac{T_p - Rdt - Mdt}{T_f + T_{de} + 1} = \frac{5000 - 50 - 300}{2 + 2 + 1} = 930 \text{ hours}$$

11. Mean time between scheduled maintenance and forced outage (MTBM)

$$MTBM = T_p / (T_f + T_{de}) = 5000 / 4 = 1250 \text{ hours}$$

12. Mean time between failures (MTBF)

$$MTBF = T_p / T_f = 5000 / 2 = 2500 \text{ hours}$$

13. Failure rate (failures per calendar year)

$$\lambda = \frac{T_f}{(T_p / 8760)} = \frac{2}{5000/8760} = 3.504 \text{ failures per calendar year}$$

14. Forced outage, failure rate (failures per operating year)

$$FR_o = \frac{T_f}{T_{op} / 8760} = \frac{2}{4650/8760} = 3.767742 \text{ failures per operating year}$$

15. Frequency of maintenance action (failures per calendar year)

$$FRc = \frac{Tma}{T_p / 8760} = \frac{2}{5000 / 8760} = 3.504 \text{ maintenance actions per operating year}$$

16. Inherent availability ( $A_i$ )

$$A_i = \frac{MTBF}{MTBF + MTTR} = \frac{2500}{2500 + 25} = 0.990099$$

17. Operational Availability ( $A_o$ )

$$A_o = \frac{MTBM}{MTBM + MDT} = \frac{1250}{1250 + 87.5} = 0.934579$$

## 5. Review of basic probability

### 5.1 Sample space

Sample space is the set of all possible outcomes of a phenomenon. For example, consider a system of three components. Assuming that each component exists either in the operating, or up, state or in the failed, or down, state, consider the sample space:

$$S = (1U, 2U, 3U), (1D, 2U, 3U), (1U, 2D, 3U), (1U, 2U, 3D), \\ (1D, 2D, 3U), (1D, 2U, 3D), (1U, 2D, 3D), (1D, 2D, 3D)$$

Where iU and iD denote that the component i is up or down, respectively. The possible outcomes of a system are also called *system states*, and the set of all possible system states is called *system state space*.

### 5.2 Event

In the example of the three-component system, the descriptions (1D, 2D, 3U), (1D, 2U, 3D), (1U, 2D, 3D), and (1D, 2D, 3D) define the events in which two or three components are in the failed state. Assuming that a minimum of two components is needed for successful system operation, this set of states (A) also defines the system failure. A is, therefore, a set of system states, and the event A(N) is said to have occurred if the system is in a state that is a member of set A.

### 5.3 Combinatorial properties of event probabilities

The following subclauses present a few basic combinatorial properties of event probabilities.

#### 5.3.1 Addition rule of probabilities

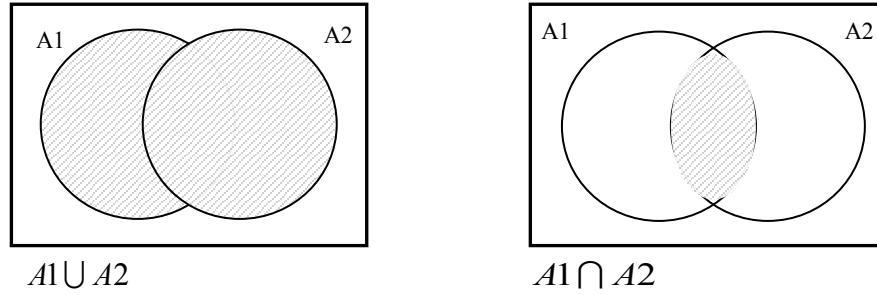
Two events, A1 and A2, are mutually exclusive if they cannot occur together. For events A1 and A2 that are not mutually exclusive (that is, events which can happen together), see Equation (1).

$$P(A1 \cup A2) = P(A1) + P(A2) - P(A1 \cap A2) \quad (1)$$

where

$P(A1 \cup A2)$  is the probability of A1 or A2, or both happening  
 $P(A1 \cap A2)$  is the probability of A1 and A2 happening together

The following Venn diagrams represent the above logical relationships graphically:



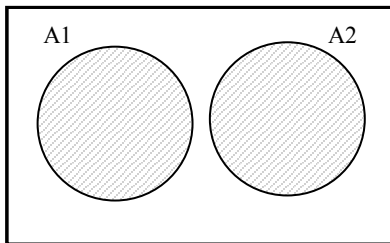
**Figure 2—Venn diagram representations of union and intersection properties**

When A1 and A2 are mutually exclusive, they cannot happen together; that is,  $P(A1 \cap A2) = 0$ , therefore Equation (1) reduces to Equation (2):

$$P(A1 \cup A2) = P(A1) + P(A2) \quad (2)$$

where

A1 and A2 are mutually exclusive (see Figure 3).



**Figure 3—Venn diagram representations of mutually exclusive events**

### 5.3.2 Multiplication rule of probabilities

If the probability of occurrence of event A1 is affected by the occurrence of A2, then A1 and A2 are not independent events.

The conditional probability of event A1, given that event A2 has already occurred, is denoted by  $P(A1 | A2)$  and Equation (3):

$$P(A1 \cap A2) = P(A1 | A2) \cdot P(A2) \quad (3)$$

Equation (4) is also used to calculate the conditional probability:

$$P(A1 | A2) = \frac{P(A1 \cap A2)}{P(A2)} \quad (4)$$

When, however, events  $A1$  and  $A2$  are independent, that is, the occurrence of  $A2$  does not affect the occurrence of  $A1$ , use Equation (5):

$$P(A1 \cap A2) = P(A1) \cdot P(A2) \quad (5)$$

### 5.3.3 Complementation

$A'1$  is used to denote the complement of event  $A1$ . The complement  $A'1$  is the set of states that are not members of  $A1$ . For example, if  $A1$  denotes states indicating system failure, then the states not representing system failure make  $A'1$  [see Equation (6) and Figure 4].

$$P(A'1) = 1 - P(A1) \quad (6)$$

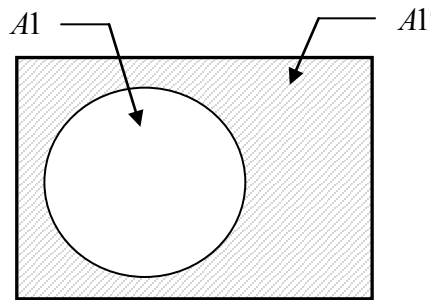


Figure 4—Venn diagram representations of an event's complement

## 5.4 Reliability and availability

In the reliability engineering discipline, the terms *reliability* and *availability* have specialized technical meanings. In general, reliability refers to system performance over time. And unfortunately, reliability is often shorthand for *reliability engineering* and its practice, results, etc. Reliability engineering is a design engineering discipline that applies scientific knowledge to assure a product will perform its intended function for the required duration within a given environment. This includes designing in the ability to maintain, test, and support the product throughout its total life cycle. This is accomplished concurrently with other design disciplines by contributing to the selection of the system architecture, materials, processes, and components—both software and hardware— followed by verifying the selections made by thorough analysis and test. Availability generally refers to the quality or state of being immediately ready for use.

### 5.4.1 General concepts

The term *reliability* refers to the notion that the system performs its specified task correctly for a certain time duration. The term *availability* refers to the *readiness* of a system to immediately perform its task—at a particular time. Both terms have precise definitions within the reliability engineering discipline and typically have specified equations or methods to provide quantitative metrics for each of them. A rocket must be very reliable for the duration of the short mission, but might not be very available as it may sit in a repair state for extended periods of time.

On the other hand, power for communications facilities needs to be highly available, implying little downtime. Where the components of the system might be unreliable, the redundancies of that system can help achieve high availability.

### 5.4.2 Reliability

The probability density function for a continuous random variable  $T$  is defined as the derivative of cumulative distribution function ( $F(t)$ ) with respect to  $t$ . The probability density function (PDF) can be used to represent relative frequency of failure times as a function of time [B9]. If the time,  $t$ , over which a system must operate and the underlying distributions of failures for its constituent elements are known, then the system reliability can be calculated by taking the integral, essentially the area under the curve defined by the PDF, from time  $t$  to infinity, as shown in Equation (7).

$$R(t) = \int_t^{\infty} f(t) dt \quad (7)$$

where

$R(t)$  is the reliability of a system from time  $t$  to infinity

$f(t)$  is the PDF

**Example 2.** Given the following PDF for the random variable  $t$ , the time to failure of a pump, what is the reliability of this pump for a 200-hour operating time?

$$PDF: f(t) = \frac{0.002}{(0.0002t + 1)^2} \quad t \geq 0$$

**Solution:**

$$R(t) = \int_t^{\infty} f(t) dt = \int_t^{\infty} \frac{0.002}{(0.0002t' + 1)^2} dt' = \left. \frac{-1}{(0.0002t' + 1)} \right|_t^{\infty} = \frac{1}{(0.0002t + 1)}$$

$$R(200) = \frac{1}{(0.0002 \times 200 + 1)} = 0.9615$$

### 5.4.3 Availability

#### 5.4.3.1 Availability assumptions

Generally in this document, availability is used as a mathematical term being either the percent of time a system is immediately ready for use, or as an instantaneous probability of the system being immediately ready for use.

Generally, availability metrics fall into two distinct subsets: *inherent availability* ( $A_i$ ) and *operational availability* ( $A_o$ ).  $A_i$  considers component failure rates and the average repair time for those components.  $A_o$  goes beyond  $A_i$  in that maintenance downtimes ( $Mdt$ ), parts procurement times, logistics, etc., are included. Although  $A_o$  provides a truer availability of a system,  $A_i$  provides a metric that is not tainted by local facility characteristics, such as spare part supplies, planned outages, etc.  $A_i$  is useful as a common metric for comparing multiple facilities and measuring particular facilities against a predetermined availability goal.

Availability analyses need to have an explicit listing of the assumptions used for each unique analysis. For example, if a facility will go down for maintenance, but the outage is not deemed critical, then that outage

might not be included in that analysis. On the other hand, if a mission-critical facility has a planned maintenance event on a redundant piece of equipment, then that planned outage could be included to capture the additional exposure to risk as the redundancy of the system is temporarily lost.

#### 5.4.3.2 Inherent availability definition

In general, availability is immediate readiness for use. For this recommended practice, we only consider  $A_i$  and calculate the metric for  $A_i$  explicitly as shown in Equation (8):

$$A_i = \frac{MTBF}{MTBF + MTTR} \quad (8)$$

where

$MTBF$  is mean time between failures

$MTTR$  is mean time to repair

If the system never failed, the  $MTBF$  would be infinite and  $A_i$  would be 1. Or, if it took no time at all to repair the system,  $MTTR$  would be zero and again the availability would be 1. Figure 5 is a graph showing availability as a function of  $MTBF$  and  $MTTR$  [availability is calculated using Equation (8)]. Note that you can achieve the same availability with different values of  $MTBF$  and  $MTTR$ . With lower  $MTBF$ , lower levels of  $MTTR$  are needed to achieve the same availability and vice versa.

#### 5.4.3.3 Inherent availability misinterpretations/limitations

Power availability metrics tend to be reported as a function of 9s. This refers to the quantity of 9s past the decimal point. A facility with an availability of 0.99999 would be referred to as having five 9s.

A common misunderstanding—and misuse—of the metric is the interpretation that a mean downtime ( $MDT$ ) can be extracted from an availability metric. For example, a common proclamation is that a facility that has achieved five 9s availability can expect an average downtime of approximately 5 min per year. It is mathematically true that the system will be down an average of 5 min per year over the long run, i.e., as  $t \rightarrow \infty$ . However, if  $MTBF$  is known, or calculated a priori, to be 87 660 h (10 y), then the expected duration of the outage will be 52 min.

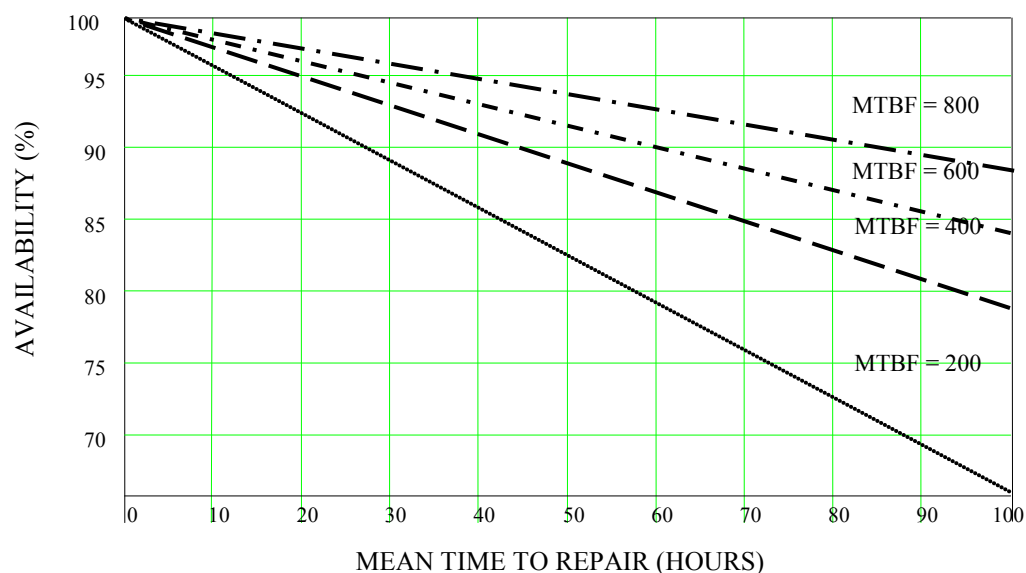


Figure 5—Different combinations of  $MTBF$  and  $MTTR$  yield the same availability



Essentially, the availability metric is a ratio of two parameters. Given an availability metric, there are infinite combinations of *MTBF* and *MTTR* metrics that can yield the same availability metric. Thus, if availability of a system is estimated through modeling, great care must be taken in extracting system *MTBF* and *MTTR* metrics.

## 5.5 Time to failure data

Time to failure data recording involves collecting time to failure of unit(s) under test. Time to failure can be attributed to a component or a system. Given that failure data can be collected in many different ways, it is important to identify the type of time to failure data before any reliability analysis.

It is assumed that each failure represents an independent sample from the same population. The population is defined as the distribution of all possible failure times and may be represented by  $f(t)$ ,  $R(t)$ ,  $F(t)$ , or  $\lambda(t)$ . The main goal of time to failure analysis is to determine the best failure distribution implied by the observed failure times in the sample.

Failure data may be classified in several ways. Among them are:

- a) Operational versus test-generated failures
- b) Grouped versus ungrouped data
- c) Large samples versus small samples
- d) Complete versus censored data

The following subclauses present some of the more common schemes of time to failure data recording as reference.

### 5.5.1 Failure times

The simplest and most common type of failure data collection is recording the length of time until a component or system fails.

### 5.5.2 Failure numbers

In this case, the number of failures after a set time is recorded. It is assumed that the failure times are unknown.

### 5.5.3 Group tests

In this case, it is assumed that multiple systems are tested in a group. When one system fails, the test is stopped, the failed unit is repaired and any necessary design changes or corrective actions are taken for the rest of the systems in the group, and the test is resumed. Then the time to failure for the failed system along with the operating times of other systems are recorded.

## 6. Defining frequency and duration of outages and interruptions, $\lambda$ , *MTBF*

The definitions and assumptions associated with frequency and duration data are critical to effectively measuring the reliability of a power system. The choice of metric used to define outages and repair times is dependent on the data used to generate the statistic, which leads to the proper distribution function (see Clause 8).

## 6.1 Frequency of failures, outages

Historically, frequency was synonymous with the failure rate (or *MTBF*), which implied the exponential distribution attribute of having a constant failure rate with randomly occurring events throughout the life of the component or system. The failure distribution of few components is random and therefore described by the exponential function. Its popularity is a function of the fact that it is the best distribution given the data that is available for most power components.

As data collection efforts continue, time to failure data, coupled with the maintenance practices on that equipment, will produce data that can be tested for best fit for multiple distributions, primarily the Weibull (see 7.5).

## 6.2 Duration of outages and interruptions

Similarly, the duration of outages has historically been described as the *MTTR*—implying the exponential distribution. This, again, was due to a lack of detailed data. In considering descriptive statistics to represent the duration of outages, the assumptions, such as the inclusion of scheduled repairs, logistics, and spare parts availability, must be explicitly stated.

## 7. Probability distributions

Probability distributions are mathematical equations that describe the probability of a particular event occurring with respect to time. For reliability analysis, what is of great interest is the probability distribution of failure. These functions capture failure characteristics such as wearout failure modes, infant mortality, random failures, etc. The most common distribution for power reliability analyses (the term *reliability* used in the general sense, as described in 6.1) is the exponential distribution. This function describes a random failure mode where the *MTBF* is the critical parameter. Other distributions include the Weibull, the Lognormal, etc.

### 7.1 Probability density functions

Each probability distribution has a unique PDF. The area under the curve of a probability density function for failure shows the relative probability of a failure event occurring before a certain time. An example of a PDF is shown in Figure 6 where  $f(t)$  is the probability density function plotted versus time ( $t$ ). The relative probability or area under the curve  $f(t)$  is called the cumulative distribution function (CDF) and is the integral of  $f(t)$  with respect to time. This integral function,  $F(t)$ , is shown in Equation (9):

$$F(t) = \int_0^t f(t)dt \quad (9)$$

where

$F(t)$  is the probability of a failure occurring before time  $t$

$f(t)$  is the PDF of failure

### 7.2 Cumulative distribution function

Plotting  $F(t)$  gives us the CDF, which shows the probability of a failure occurring at time  $t$  (see Figure 7).

Finally, the reliability function  $R(t)$  is the probability of a component not failing by time  $t$ .

Therefore  $R(t) = 1 - F(t)$ .

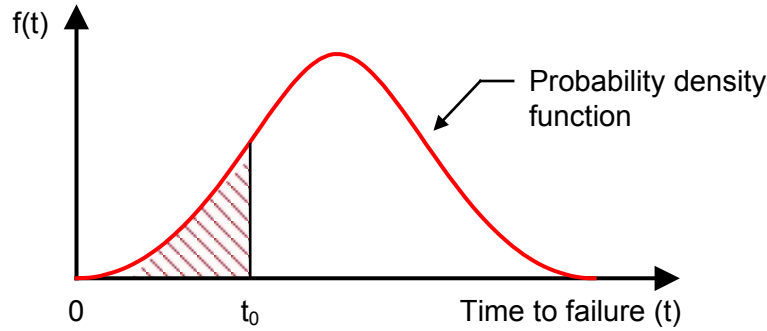


Figure 6—Probability of a failure represented by the area under the curve of the PDF

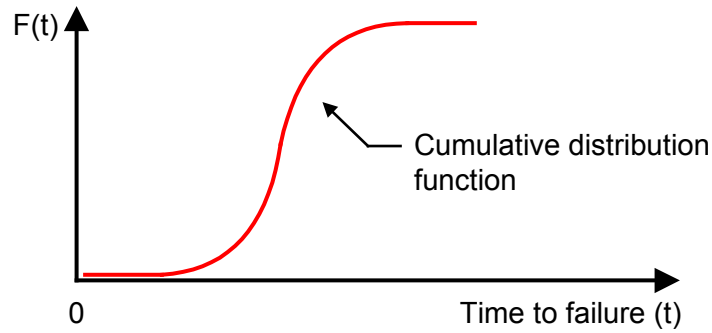


Figure 7—The cumulative distribution

### 7.3 Hazard function

The hazard function, or hazard rate, is the instantaneous failure rate for the remaining population of interest at time  $t$ . It is denoted as shown in Equation (10):

$$H(t) = \frac{f(t)}{R(t)} \quad (10)$$

### 7.4 Exponential distribution

The PDF for the exponential distribution is shown in Equation (11):

$$f(t) = \lambda e^{-\lambda t} \quad (11)$$

Thus, the CDF is shown in Equation (12):

$$F(t) = 1 - e^{-\lambda t} \quad (12)$$

And the reliability function is shown in Equation (13):

$$R(t) = e^{-\lambda t} \quad (13)$$

where

$\lambda$  is the failure rate (inverse of *MTBF*)  
 $t$  is the length of time the system must function  
 $e$  is the base of natural logarithms

It can be seen that the hazard function is as shown in Equation (14):

$$H(t) = \frac{\lambda e^{-\lambda t}}{e^{-\lambda t}} = \lambda \quad (14)$$

This is to be expected, as the instantaneous failure rate is constant for the exponential distribution.

The most essential characteristic of the exponential distribution, which is the common PDF in availability analyses, is that the failure rate is constant over time—the component is no more likely to fail in its first year of life than it is in its 21st year of life. It should not be assumed that all components exhibit this characteristic. Most do not. Its popularity is a function of the fact that it is the best PDF given the data that supports the reliability metrics of most power components. Essentially, the exponential requires only the *MTBF*, which can be easily determined by a total component run time and a total of component failure events.

**Example 3.** A compressor has a constant failure rate  $\lambda = 3.2 \times 10^{-4}$  (hours<sup>-1</sup>). What is the probability that this compressor survives two months of operation?

**Solution:**

$$R(2 \times 30 \times 24) = R(1440) = e^{-3.2 \times 10^{-4} \times 1440} = 0.631.$$

## 7.5 Weibull distribution

The Weibull distribution is one of the most widely used in life data distribution analysis. It is a versatile distribution that can take on the characteristics of other types of distributions based on the value of the shape parameter beta ( $\beta$ ). When  $0 < \beta < 1$ , the Weibull distribution is a decreasing failure rate distribution which can be used to describe burn-in (early) type failure behavior. For  $\beta = 1$ , the Weibull distribution reduces to the exponential distribution. If  $\beta > 1$ , the Weibull distribution can be used as a model for the wearout region of the bathtub curve (as an increasing failure rate distribution). The eta ( $\eta$ ) parameter is a location parameter. Where the beta parameter tells us how the part is going to fail, the eta parameter tells us when.

### 7.5.1 PDF and CDF

Equation (15) shows the Weibull PDF:

$$f(t, \beta, \eta) = \frac{\beta}{\eta} \left( \frac{t}{\eta} \right)^{\beta-1} e^{-\left( \frac{t}{\eta} \right)^{\beta}} \quad (15)$$

where

$\beta$  is the shape parameter  
 $\eta$  is the location parameter

Equation (16) shows the Weibull CDF:

$$F(t, \beta, \eta) = 1 - e^{-\left(\frac{t}{\eta}\right)^\beta} \quad (16)$$

The reliability function for the Weibull distribution is shown in Equation (17):

$$R(t) = e^{-\left(\frac{t}{\eta}\right)^\beta} \quad (17)$$

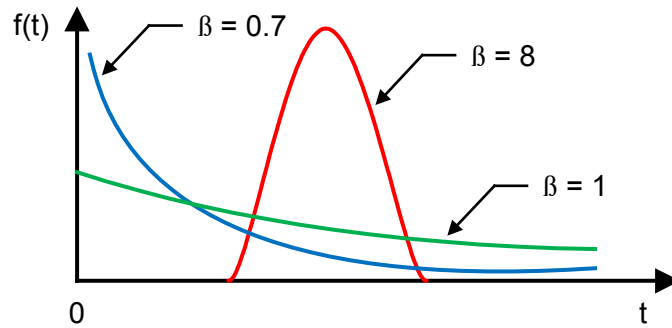
The hazard function for the Weibull distribution is shown in Equation (18):

$$H(t, \beta, \eta) = \beta \cdot t^{\beta-1} \quad (18)$$

When  $\beta = 1$ , the Weibull distribution is equal to the exponential distribution, as shown in Equation (19):

$$f(t, 1, \eta) = \frac{1}{\eta} e^{-\left(\frac{t}{\eta}\right)} \quad (19)$$

Note the variety in PDF shapes depending on the choice of  $\beta$ , as shown in Figure 8.



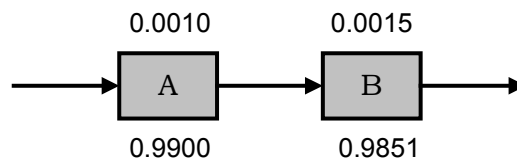
**Figure 8—Variation of the beta parameter**

## 7.6 Calculating reliability for the exponential distribution

If the underlying distribution for each element is exponential and the failure rates,  $\lambda_i$ , for each element are known, then the reliability of the system can be calculated using Equation (13).

### 7.6.1 Series reliability

Consider the system represented by the reliability block diagram (RBD) in Figure 9.



**Figure 9—Example reliability block diagram**

NOTE—The number above each block in Figure 9 is the failure rate  $\lambda$  in failures per million hours. The inverse of the failure rate is the *MTTF* (exponential failure rate assumed). The number below each block is the reliability calculated using Equation (13) with  $t = 10$  million hours.<sup>5</sup>

### 7.6.1.1 Series configuration—weakest link

Components A and B in Figure 9 are said to be in series, which means all must operate for the system to operate. Since the system can be no more reliable than the least reliable component, this configuration is often referred to as the *weakest link configuration*. An analogy would be a chain; the strength of the chain is determined by its weakest link.

### 7.6.1.2 Series calculation method 1

Since the components are in series, the system reliability can be found by adding together the failure rates of the components. The system failure rate is  $\lambda = 0.0010 + 0.0015 = 0.0025$  per million hours. The reliability is shown in Equation (19) for  $t = 10$  million hours:

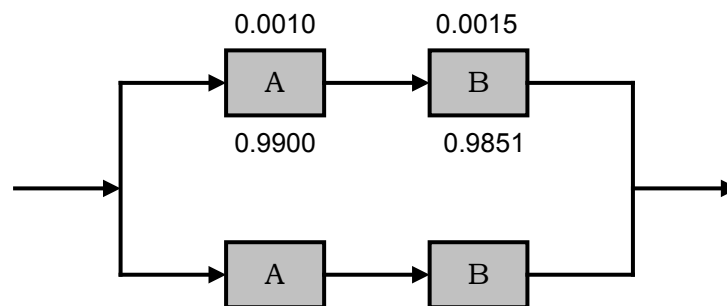
$$R(t) = e^{-\lambda t} = e^{-0.0025 \times 10} = 0.9753 \quad (19)$$

### 7.6.1.3 Series calculation method 2

Alternatively, we could find the system reliability by multiplying the reliabilities of the two components as follows:  $0.9900 \times 0.9851 = 0.9753$ .

## 7.6.2 Reliability with redundancy

Now consider the RBD shown in Figure 10.



**Figure 10—RBD of a system with redundant components**

NOTE—The number above each block in Figure 10 is the failure rate in failures per million hours. The inverse of the failure rate is the *MTTF* (exponential failure rate assumed). The number below each block is the reliability.

The system represented by the block diagram in Figure 10 has the same components (A and B) used in Figure 9, however, two of each component are used in a configuration referred to as *redundant* or *parallel*. Two paths of operation are possible. The paths are top A-B or bottom A-B. If either of two paths is intact, the system can operate. The reliability of the system is most easily calculated by finding the probability of failure ( $1 - R(t)$ ) for each path, multiplying the probabilities of failure (which gives the

<sup>5</sup> Notes in text, tables, and figures of a standard are given for information only and do not contain requirements needed to implement this standard.

probability of both paths failing), and then subtracting the result from 1. The reliability of each path was found in the previous example. Next, the probability of a path failing is found by subtracting its reliability from 1. Thus, the probability of either path failing is  $1 - 0.9753 = 0.0247$ . The probability that both paths will fail is  $0.0247 \times 0.0247 = 0.0006$ . Finally, the reliability of the system is  $1 - 0.0006 = 0.9994$ , a significant improvement over the series-configured system, which had a reliability of 0.9753.

### 7.6.3 N + X redundancy

System redundancy is not restricted to simply having twin systems. Where N is defined as the required piece of equipment to achieve an operational system, 2N would, in turn, imply that there is double the capacity, i.e., 1 of 2 would be required to operate for system success. In some facilities, where there is a full 2N philosophy for redundancy, the facility will often have one additional piece of equipment on each side so that if one of the N pieces of equipment is down for maintenance, the facility still is 2N redundant. This would be the  $2(N + 1)$  configuration.

With respect to availability, the following tables represent the availability of a system that requires 1000 kVA of power, assuming that each has an availability of 0.99.

Case 1: Use 1000 kVA generators  $\rightarrow N = 1$

Number of generators	Redundancy	Requirement	Availability
1	N	1 of 1	0.99
2	N + 1	1 of 2	0.9999
3	N + 2	1 of 3	0.999999

Case 2: Use 500 kVA generators  $\rightarrow N = 2$

Number of generators	Redundancy	Requirement	Availability
2	N	2 of 2	0.98
3	N + 1	2 of 3	0.9997
4	N + 2	2 of 4	0.999996

Case 3: Use 250 kVA generators  $\rightarrow N = 4$

Number of generators	Redundancy	Requirement	Availability
4	N	4 of 4	0.96
5	N + 1	4 of 5	0.9990
6	N + 2	4 of 6	0.99998

### 7.6.4 k of n calculations for reliability

Equation (20) can be used for calculating the reliability of  $k$  or more successes from  $n$  components for any arbitrary  $k$  or  $n$ :

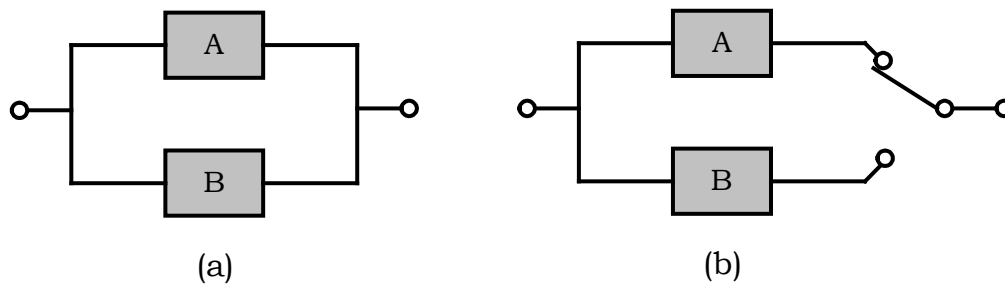
$$R(t) = \sum_{x=k}^n \frac{n!}{x!(n-x)!} e^{-\lambda x t} (1 - e^{-\lambda t})^{(n-x)} \quad (20)$$

where

$n$  is the total number of components  
 $k$  is the required components

### 7.6.5 Standby redundancy with perfect vs. imperfect switch

Figure 11 (a) presents a parallel redundant system in which both component A and component B are in service and carrying load. Upon failure of one component, the other will continue carrying the load without any interruption [B2] and [B3].



**Figure 11—Redundancy models (a) parallel redundancy and (b) standby redundancy**

Figure 11 (b) shows a standby redundant system in which component A is carrying the load, and component B is idle until the switching mechanism senses that component A has failed. Then the switching system transfers the load to component B. Assume the switch is perfect and it will not fail to transfer to standby system and will not fail during the operation. To analyze the probability of system failure, again, assuming that component B will not fail while in standby, the system will fail only when component A fails; and component B fails given that component A has already failed. The probability of system failure will be:

$$(1 - R(\text{system})) = [1 - R(A)] \times [1 - R(B | A')] \quad (21)$$

If we assume component A and B are independent,

$$(1 - R(\text{system})) = [1 - R(A)] \times [1 - R(B)] \quad (22)$$

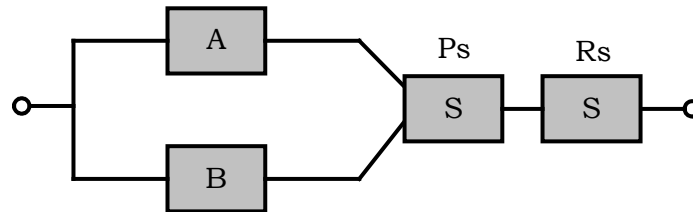
which would be the same as if component A and component B were parallel redundant. The numerical results, however, will not be the same because the reliability indices of a standby component are different for the same component when operating in parallel redundant mode.

In case of imperfect switch, the switch has a probability of failure to transfer to a standby component. Let the probability of successful transfer to standby component be  $P_s$  and the probability of unsuccessful transfer be  $P_{s'} = (1 - P_s)$ . Now the probability of system failure can be described as

$$P(\text{sys failure}) = P(\text{sys failure} | \text{successful transfer}) \times P(\text{successful transfer}) \\ + P(\text{sys failure} | \text{unsuccessful transfer}) \times P(\text{unsuccessful transfer}) \quad (23)$$



Additionally, in an imperfect switch, there is a possibility of failure in its initial operating position as well as failing to transfer when required. Given that failure of the switch in its operating is likely to be same whether it is connected to component A or B, then this failure mode can be modeled in series with the parallel path formed by components A and B. Consequently, in the block diagram of Figure 11 (b), the switch can be replaced with two blocks as shown in Figure 12, one representing the probability of successful change over ( $P_s$ ) and the other the reliability of the switch in its initial operating position ( $R_s$ ).



**Figure 12—Standby redundancy with imperfect switch [B2], [B3]**

## 8. Methods of reliability and availability analysis

The following subclauses present two broad categories of reliability and availability analysis: qualitative analysis and analytical/numerical methods. For each group, extensive lists of methodologies are presented and a selected number of them explored in more detail. Clause 10 follows and provides general comparison of the various reliability and availability analysis methods.

### 8.1 Qualitative system analysis

The main goal of the reliability engineer is to identify potential failures and make considerations to prevent these failures. We define the failure of a functional block—that could be a component, sub-system, or a system—as the termination of its ability to perform its intended function. Therefore, the relevant functions and the performance criteria related to each function need to be identified. There are various methods to analyze these functions.

#### 8.1.1 Fault tree analysis

Fault tree analysis (FTA) is a top-down deductive approach to failure analysis, starting with a potential undesirable event called a TOP event, then determining all the causes that may contribute to the TOP event. This qualitative approach may be followed by a quantitative analysis to estimate the probability of occurrence of a TOP event.


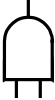




A fault tree analysis is typically carried out in six steps:

- a) Definition of the system, the TOP event (the potential accident), and the boundary conditions
- b) Construction of the fault tree
- c) Identification of the minimal cut sets
- d) Qualitative analysis of the fault tree
- e) Quantitative analysis of the fault tree
- f) Reporting of results

The critical event to be analyzed is typically called the TOP event. The description of this event should answer to the questions what, where, and when [B1]. What describes the type of critical event (i.e., transformer oil leak). Where describes the location of the critical event (i.e., leak at the bottom of transformer radiator). And finally, when describes the time of the critical event (i.e., transformer leak during the maintenance). In addition, the boundary conditions such as physical conditions, initial condition, type of external stresses, etc. need to be identified.

Construction of fault tree starts from the TOP event. The next layer of the tree is made of all fault events that are immediate, necessary, and sufficient cause to result in the TOP event. This process is continued all the way down to the basic events. Table 4 presents typical fault tree symbols.

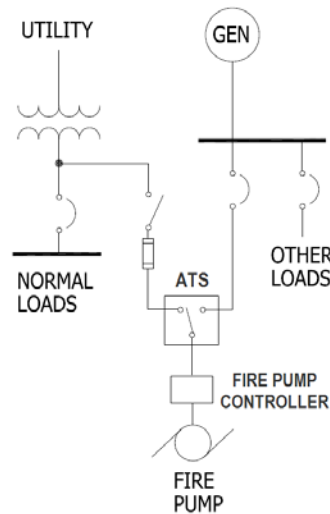
**Table 4—Fault tree symbols**

OR gate		The OR gate indicates that output event occurs if any of the inputs occur.
AND gate		The AND gate indicates that output event occurs if all of the inputs occur.
Basic event		The basic event represents one of the lowest level component failure events that does not require any further failure cause analysis.
Description		The comment rectangle is used for supplementary information.
Transfer symbols	<div style="display: flex; justify-content: space-around; align-items: center;"> <div style="text-align: center;">  Transfer out </div> <div style="text-align: center;">  Transfer in </div> </div>	Transfer out symbol indicates that the fault tree has developed further at the point of transfer in symbol.

A cut set in a fault tree is a set of basic events whose occurrence (simultaneously) ensures that the TOP event occurs. A cut set is said to be minimal if the set cannot be reduced without losing its status as a cut set. Therefore, the TOP event will occur if all the basic events in a minimal cut set occur at the same time. A qualitative assessment of the fault tree comprises of reviewing the minimal cut sets and perhaps ranking them based on their order of criticality.

The quantitative assessment of fault tree involves calculating the probability of occurrence of the TOP event based on the prior knowledge of basic events failure probabilities.

**Example 4.** Figure 13 illustrates the electrical one-line diagram of a typical fire pump power system with utility, on-site diesel engine generator, and automatic transfer switch (ATS) providing power to a fire pump [B1].



**Figure 13—Fire pump power system one-line diagram**

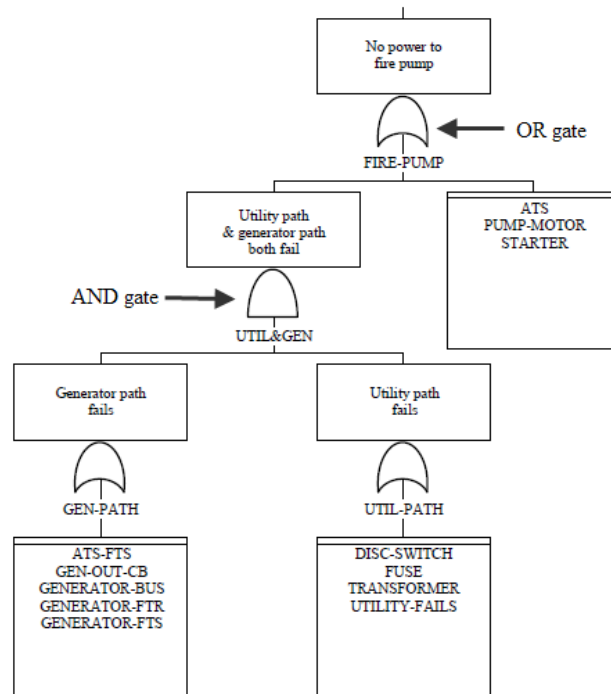
- Draw the fault tree of this system assuming the TOP event being the loss of power to the fire pump.
- Utilize the data set provided in Table 5 and perform a quantitative fault tree analysis and calculate the probability of failure for TOP event after one year. Assume the probability of a diesel engine generator not starting upon a start command being 0.00606 and the probability of the ATS not transferring when required to be 0.01.

**Table 5—Failure and repair data set for fire pump power system**

Part description	MTBF (hours)	MTTR (hours)
Utility power—single	4478.5	1.32
Utility power—two independent sources	28 077	0.52
Transformer	2 642 019	37.23
Fused disconnect	3 829 588	3.95
Generator	545.1	4.10
Circuit breaker	2 644 087	1.52
ATS	101 642	5.73
Motor and starter	348 699	7.96

**Solution:**

- Figure 14 presents the fault tree of the fire pump power system.



**Figure 14—Fault tree of fire pump power system**

b) Table 6 presents the cut set report of fire pump power system fault tree.

**Table 6—Cut set report for fault tree of Figure 14**

Cut #	Cut set %	Probability/frequency	Basic event	Description	Probability
1	67	8.30E-02	ATS	ATS1: ATS	8.30E-02
2	30	3.70E-02	GENERATOR-FTR	GEN3: GENERATOR FAILS TO RUN	4.30E-02
			UTILITY-FAILS	UTL: UTILITY SINGLE CIRCUIT	8.60E-01
3	4.2	5.20E-03	GENERATOR-FTS	GENERATOR FAILS TO START	6.10E-03
			UTILITY-FAILS	UTL: UTILITY SINGLE CIRCUIT	8.60E-01
4	1.5	1.80E-03	STARTER	MAGNETIC MOTOR STARTER FAILS	1.80E-03
5	0.4	4.30E-04	ATS-FTS	ATS FAILS TO SWITCH	5.00E-04
			UTILITY-FAILS	UTL: UTILITY SINGLE CIRCUIT	8.60E-01
6	0.1	1.40E-04	GENERATOR-FTR	GEN3: GENERATOR FAILS TO RUN	4.30E-02
			TRANSFORMER	XFMR1: TRANSFORMER < 600 V (FMEA)	3.30E-03
7	0.1	9.80E-05	FUSED-DSW	FUSED DISCONNECT SWITCH	2.30E-03
			GENERATOR-FTR	GEN3: GENERATOR FAILS TO RUN	4.30E-02

**Table 7—Fault tree analysis results for fire pump power system**

Description of fault tree	Probability of failure (1 year)	Unavailability	Availability
Power to fire pump—single utility and generator	12.33%	0.00010770	0.9998923

Table 7 shows the summary of fault tree analysis using reliability software to calculate the unreliability (probability of failure) and unavailability of the power system of fire pump.

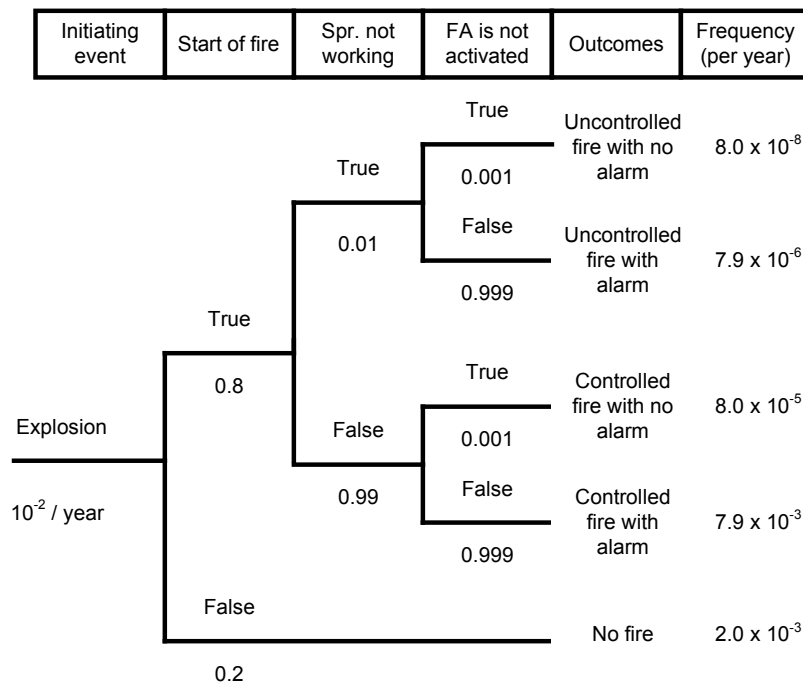
### 8.1.2 Event tree analysis

An event tree analysis (ETA) is a procedure that shows all possible outcomes resulting from an initiating event. It displays a chronological development of event chains starting with the initiating event and proceeding all the way through success and failures in response to the initiating event. The event tree diagram is drawn from left to right starting with an initiating event followed by various nodes, each related to an event. When data related to the initiating event and following success and failures are available, a quantitative analysis of the event tree can be performed to calculate the probabilities and frequencies of the resulting consequences.

To construct an event tree, the following steps need to be taken [B16]:

- Identify a relevant initial event that may cause unwanted consequences
- Identify the barriers that are designed to deal with the accidental event
- Construct the event tree
- Describe the (potential) resulting accident sequences
- Determine the frequency of the accidental event and the probabilities of the branches in the event tree
- Calculate the probabilities/frequencies for the identified consequences (outcomes)
- Compile and present the results from the analysis

**Example 5.** The following event tree from IEC 60300 shows the details of the above steps in an example.



**Figure 15—Event tree example from IEC 60300 3-9**

### 8.1.3 Failure mode, effect, and criticality analysis (FMECA)

This is a methodology to identify and analyze all potential failure modes of the various parts of a system, the effects these failures may have on the system, and how to avoid the failures, and/or mitigate their

effects on the system. FMECA is a technique used to identify, prioritize, and eliminate potential failures within a system. Initially, the FMECA was called FMEA (failure modes and effects analysis). The C in FMECA indicates that the criticality (or severity) of the various failure effects are considered and ranked. FMECA was one of the first systematic techniques for failure analysis. FMECA was developed by the U.S. military and the first guideline was Military Procedure MIL-P-1629, Procedures for performing a failure mode, effects and criticality analysis, dated November 9, 1949 [B16]. FMECA is the most widely used reliability analysis technique in the initial stages of product/system development.

There are two approaches in developing FMECA: bottom-up approach and top-down approach. The bottom-up approach is used when a system concept has been designed and all the components have been studied. The top-down approach is used when the system is in the early stages of design and all the components have not been finalized yet. This approach is function oriented and the analysis starts with the main system function that might fail. Then functional failures with major effects are prioritized.

MIL-STD 1629, IEC 60812, and BS 5760-5 can be used as reference for FMECA.

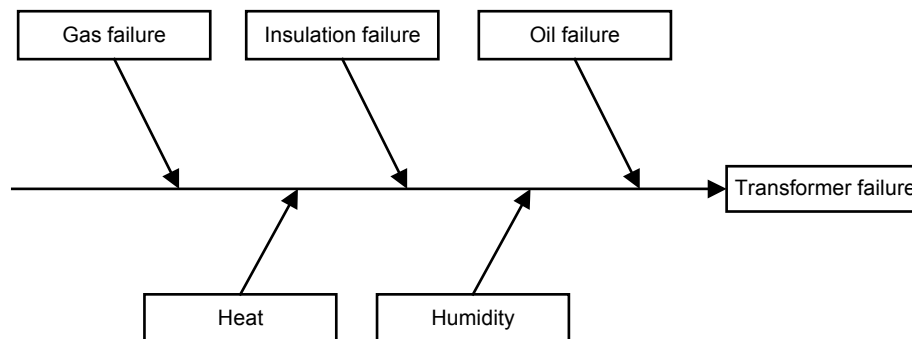
Figure 16 shows an example of FMECA worksheet.

Description of unit			Description of failure			Effect of failure		Failure rate	Severity ranking	Risk reducing measures	Comments
Ref. No.	Function	Oper. Mode	Failure mode	Failure cause or mechanism	Detection of failure	On the subsystem	On the system function				

**Figure 16—An example of FMECA worksheet**

#### 8.1.4 Cause and effect diagrams

A cause and effect diagram is a graphical tool frequently used by quality engineers to identify, sort, and display possible causes of a problem or quality characteristic. It helps determine root causes, encourages group participation, uses an orderly, easy-to-read format, indicates possible causes of variation, increases process knowledge, and identifies areas for collecting data. Cause and effect diagrams are qualitative and cannot be used as tools for quantitative analysis. There are various types of cause and effect diagrams. One example, is a fishbone diagram, as shown in Figure 17.



**Figure 17—An example of a cause and effect diagram**

### 8.1.5 Bayesian belief networks

Bayesian belief network (BBN) or Bayesian network (BN), also known as Bayesian net, is a graphical modeling tool for specifying probability distributions that uses directed graphs together with associated set of probability tables. These graphical structures are used to represent knowledge about a system. In particular, each node in the graph represents a random variable, while the edges between the nodes represent probabilistic dependencies among the corresponding random variables.

A BBN is a compact representation of the joint probability distribution of the various system variables. Formally, it is known as a directed acyclic graph (DAG) with nodes connected by arcs. The nodes are random variables whose values represent the observed or unobserved system variables. The arcs represent the causal relationship between variables. They are quantified by the conditional probabilities that a child node would reach to a certain value, given values of all its parent nodes

BBN can also be used to represent the generic knowledge of a domain expert and to function as a computational architecture for storing factual knowledge and manipulating the flow of knowledge in the network structure. The graph structure in the network significantly reduces the storage required for the joint probability distribution and the computational burden associated with the inference process.

Figure 18 shows the Bayesian network of a partial transformer fault tree.

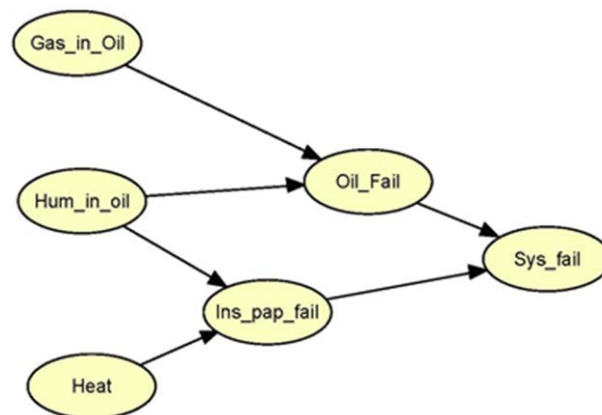
#### Abbreviations:

Hum\_in\_oil: Humidity in oil

Oil\_Fail: Oil failure

Sys\_Fail: System failure

Ins\_pap\_Fail: Insulation paper failure



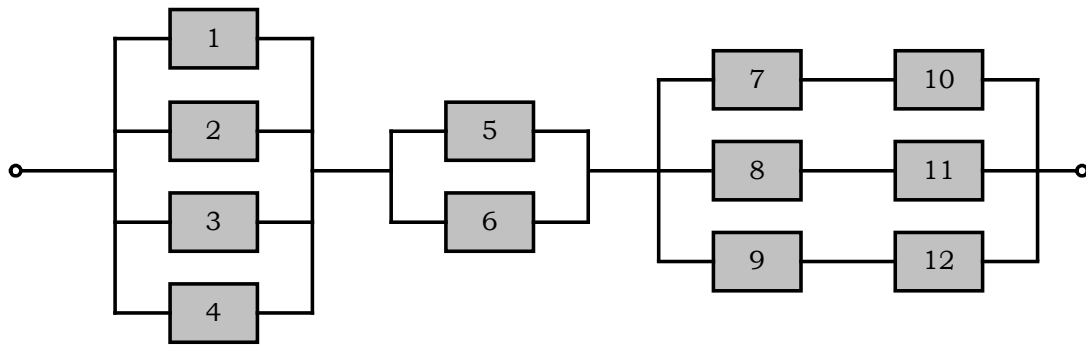
**Figure 18—An example of Bayesian network**

### 8.1.6 Reliability block diagram

Reliability block diagram (RBD) is a graphical (and analytic) tool used to model simple and complex systems. It is made of groups of blocks in series and parallel. Once the blocks are configured properly and relevant data are provided, the failure rate, MTBF, reliability, and availability of the system can be calculated. An RBD is a success oriented network and from a qualitative stand point, represents how the functioning of various blocks may fulfill the successful operation of the system.

Reliability block diagrams are suitable for analysis of non-repairable components and where the order of failures is not important. When the components are repairable and the order of failures is important, Markov method is a more suitable tool for analysis.

Figure 19 shows a simple reliability block diagram with series and parallel blocks.



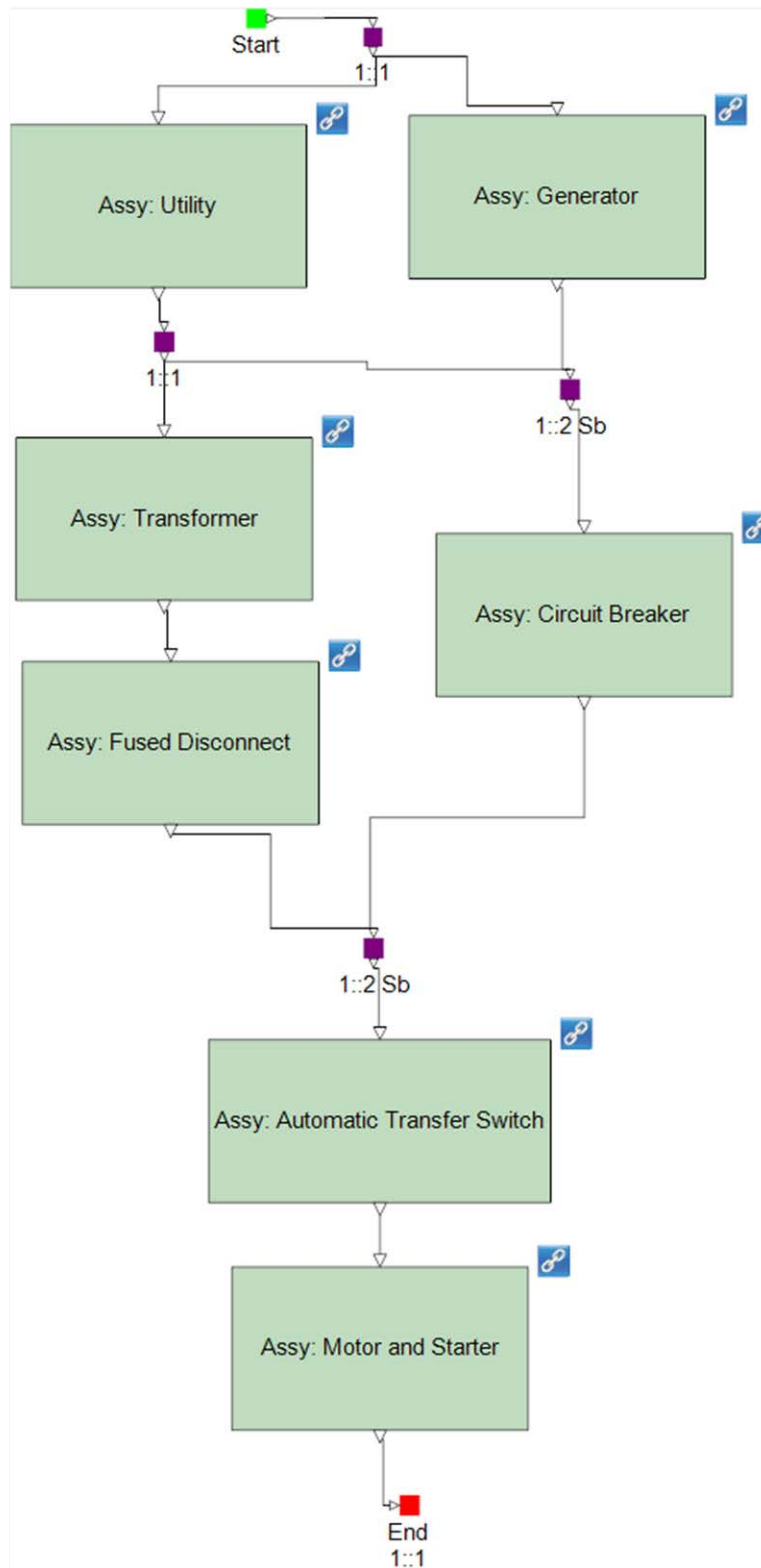
**Figure 19—A reliability block diagram**

**Example 6.** Repeat example 4 (fire pump power system) utilizing a reliability block diagram. Compare the results with the solution by fault tree analysis.

**Solution:**

Figure 20 presents the reliability block diagram of fire pump power system example.





**Figure 20—Fire pump power system reliability block diagram**

Utilizing RBD software tools, the availability and probability of failure of the power system of fire pump have been summarized in Table 8.

**Table 8—Reliability block diagram analysis results for fire pump power system**

Description of RBD	Probability of failure (1 year)	Availability
Power to fire pump—single utility and generator	12.47%	0.9999169

Comparing the results in Table 7 with Table 8, it is obvious that analysis from two different methods (fault tree and RBD) produced extremely close results.

The fundamental difference between fault tree diagrams and reliability block diagrams is that the fault trees focus on failure paths and RBDs focus on success. The fault trees look at failure combinations while RBDs look at success combinations. In addition, fault trees typically deal with fixed probabilities while RBDs may include time varying distributions. Lastly, it is almost always easy to generate a fault tree from a reliability block diagram; however, it may not be always possible to generate a reliability block diagram from a fault tree.

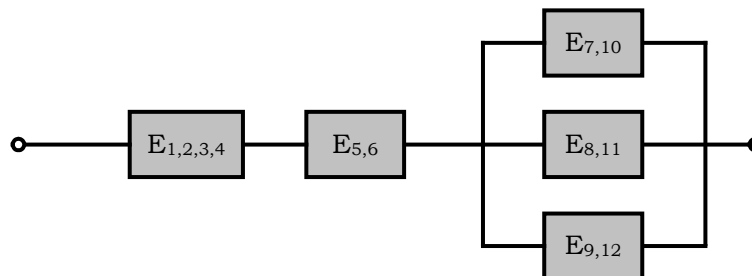
### 8.1.7 Network reduction

The network reduction method is useful for systems consisting of series and parallel subsystems. This method consists of successively reducing the series and parallel structures by equivalent components. Knowledge of the series and parallel reduction formulas is essential for the application of this technique.

**Example 7.** Using network reduction techniques, simplify (reduce) the reliability block diagram presented in Figure 19.

**Solution:**

Blocks 1, 2, 3, and 4 are in parallel and can be replaced with an equivalent block  $E_{1,2,3,4}$ . Similarly, block 5 and block 6 are in parallel and can be replaced with their equivalent block  $E_{5,6}$ . Block 7 and block 10 are in series and can be replaced with their equivalent block  $E_{7,10}$ . Similarly  $E_{8,11}$  and  $E_{9,12}$  can be replaced. The next iteration of the reliability block diagram is presented in Figure 21.



**Figure 21—A reduced version of reliability block diagram presented in Figure 19**

Similarly, blocks  $E_{1,2,3,4}$  and  $E_{5,6}$  are in series and can be replaced with their equivalent; and blocks  $E_{7,10}$ ,  $E_{8,11}$ , and  $E_{9,12}$  are in parallel and can be replaced with their equivalent. The technique can be followed until the network cannot be simplified further.

### 8.1.8 GO algorithm

The GO algorithm, a success-oriented system analysis technique, was originally developed for defense industry applications in the early 1960s. The capability of the GO methodology was drastically improved under the sponsorship of the Electric Power Research Institute (EPRI) with the development of additional analytical techniques (i.e., system interactions, system dependencies, and man-machine interactions) and

improved computer software reliability. The popularity of the GO method can be linked to basic characteristics that fault trees do not possess, including: 1) hardware is modeled in a manner more or less the same way as in the system drawings, 2) model modifications can be easily introduced to reflect configuration changes, and 3) the modeling capability is extremely flexible. GO's success-oriented technique analyzes system performance through straightforward inductive logic. The GO representation of a system, or GO model, can often be constructed directly from engineering drawings, which makes GO a valuable tool for many applications since it is relatively easy to build and review models.

A system model is first constructed within the GO methodology using a top-down (forward-looking) approach to identify the functions required for successful operation following normal process flow or operational sequences. Secondly, in the GO methodology each of the systems that provide the functionality is modeled to the required level of detail. The level of detail may be at the system, subsystem, or component level depending upon the type of information required and the plant-specific information available. The GO models determine all system-response modes: successes, failures, prematures, etc.

GO models consist of arrangements of GO operator symbols and represent the engineering functions of components, subsystems, and systems. The models are generally constructed from engineering (one-line) drawings by replacing engineering elements (valves, motors, switches, etc.) with one or more GO symbols that are interrelated to represent system functions, logic, and operational sequences. The GO software uses the GO model to quantify system performance. The method evaluates system reliability and availability, identifies fault sets, ranks the relative importance of the constituent elements, and places confidence bounds on the probabilities of occurrence of system events reflecting the effects of data uncertainties.

Some key features of the GO method are as follows:

- a) Models follow the normal process flow
- b) Most model elements have one-to-one correspondence with system elements
- c) Models accommodate component and system interactions and dependencies
- d) Models are compact and easy to validate
- e) Outputs represent all system success and failure states
- f) Models can be easily altered and updated
- g) Fault sets can be generated without altering the basic model
- h) System operational aspects can be incorporated
- i) Numerical errors due to pruning are known and can be controlled

The GO procedure uses a set of 17 standard logical operators to represent the logic operation, interaction, and combination of physical equipment and human actions. For example, a type 1 operator represents the logical operation of equipment that either performs, or fails to perform, its function given a proper input or stimulus. The type 2 operator performs the logical OR gate operation where a successful response is generated if any of several inputs is proper, etc. The random variables of the GO methodology include operator inputs called *stimuli* ( $S_1, S_2, \dots, S_n$ ) and outputs referred to as *responses* ( $R_1, R_2, \dots, R_n$ ). An operator, which represents equipment responses or human actions and which may itself have associated performance probabilities, processes the input random variable in a prescribed and well-defined way to generate the output random variables. These random variables are given the electrical term *signals* in the GO models.

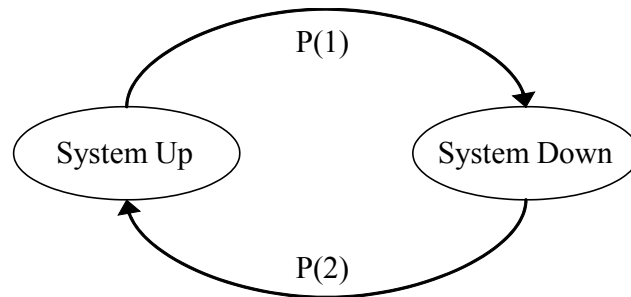
## 8.2 Numerical methods

The intent of the methods discussed in this subclause—and the entire recommended practice—is to perform reliability and availability analyses for systems. Certain functions, particularly those resulting from

exponential failure distributions, are directly applicable to one family of analyses: analytical. The probability density functions introduced in Clause 7 can be used to their greatest potential in using numerical analyses such as Monte Carlo simulation. These methods will be explored further in this subclause.

### 8.2.1 State space

The state space methodology is founded on a more general mathematical concept called Markov chains. Markov chains are a modeling technique that describes a system by the possible states which it can possess (i.e., state space). For our purpose, a system essentially resides in two distinct states: up or down. The probability of transitioning from one state to the other in a given time period is the critical reliability metric that we are after. Figure 22 shows this simple Markov model.



**Figure 22—Simple Markov model**

where

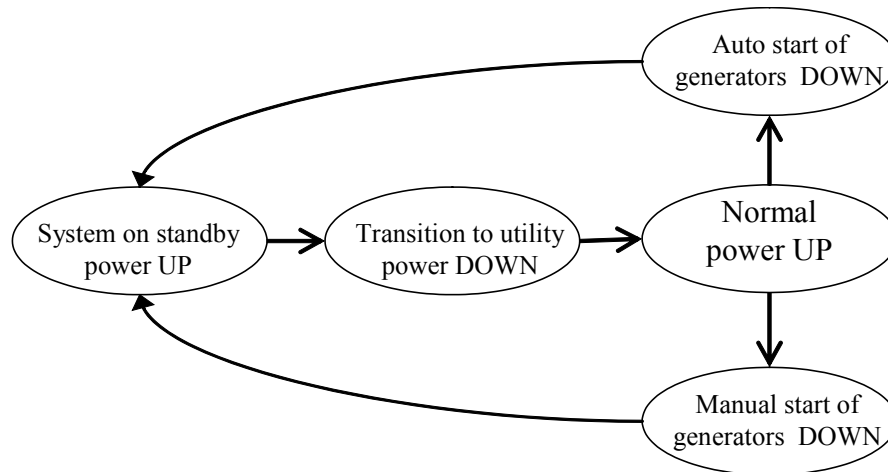
$P(1)$  is the probability of the system going down in time  $t$

$P(2)$  is the probability of the system coming up in time  $t$

However, the true goal of availability analysis is to determine the probability of being in the up state—or the time spent in the up state for a given time  $t$ . To show this, consider the simpler scenario including only a system with backup generation. Given loss of utility power, the generators will either start automatically, or if that functionality fails, the generators can be started manually. In those starting phases, the system is down. Once started, the system is up. The system will then switch to utility power once available. The system could be down during that switching.

Figure 23 shows the associated Markov model for this system. Between each of the possible states are state transitional probabilities that must be known. The solution to the model will be the time spent in the up states vs. the down states.

Solving Markov models is simple only for very simple models, by solving a set of linear equations. The complexity solving these models grows exponentially as the sizes of the models grow linearly. Solutions can be found by using complex numerical analysis methods involving linear algebraic matrix operations, etc. Markov models can also be solved by Monte Carlo techniques described as follows.



**Figure 23—Less simple Markov model**

## 8.2.2 Monte Carlo simulation

Monte Carlo simulation is the most versatile modeling methodology available. The methodology can be implemented in many forms from simple models in a spreadsheet environment to complex models that are handcrafted in a programming language of choice. There are also a variety of simulation software packages that provide drag-and-drop environments that can automate the creation of simulated models for the casual analyst.

### 8.2.2.1 Simulation basics

The Monte Carlo simulator operates on an iterative process where each iteration represents a description of what the system could experience through a set mission life. For instance, if we consider the past experience of a system, including what really failed, that experience was only one of infinite possible outcomes that depended on the failure characteristics of that system.

Thus, Monte Carlo simulation looks forward by considering possible scenarios that could occur in the future—and those scenarios, with their associated likelihoods, is dependent on the failure characteristics applied to the system components. For each iteration, failure times and the associated repair attributes are picked for each component in the system. The simulation will then implement the logical relationships of the system to determine the following:

- a) If a failure has occurred in the system prior to the defined mission life.
- b) If a failed component(s) takes the system down, what is the duration of downtime?

With these items determined, the availability for the system in that particular iteration can be calculated. Then, as this single iteration is repeated, an average is tabulated of uptime vs. downtime as well as an average of downtime durations.

## 9. Performing reliability and availability analyses

The results of availability analyses are extremely sensitive to factors such as underlying assumptions, techniques for calculating availability, and the data used to support the analysis. No results of an analysis should be distributed—let alone trusted—without documentation supporting those attributes. Subtle

differences in those attributes can produce drastically different results, results that might be used to drive design decision making. It is the ultimate responsibility of the analyst to be aware of those sensitivities and perform and present analyses with integrity.

## 9.1 Modeling limitations

Cut-set, state space, network reduction, and Boolean algebra are techniques that lend themselves to the casual reliability engineer to analyze small systems, primarily because they can all be accomplished with common desktop PC tools such as spreadsheets, etc. A series of studies recently performed on the *Gold Book Standard Network* have shown that, provided that the assumptions are held equal, each technique produces similar results.

### 9.1.1 Network size

As larger systems are modeled, the sheer size of the analysis becomes burdensome for the analyst. Furthermore, what-if sensitivity analyses also become impractical.

### 9.1.2 Smarter distributions

Data collection efforts have expanded the analysts' tools beyond the classical MTBF analysis. Failure distributions such as the normal, lognormal, Weibull, etc., are being fitted to common failure modes of many critical components in power distribution networks.

### 9.1.3 Modeling obstacles

There are several system attributes that are challenging to model. UPS battery life, for instance, had historically been assumed to be limitless in many analyses, whereas their contribution to power availability is not. Furthermore, data have shown that standby equipment has differing distributions from its primary counterparts. Thirdly, spare parts availability, human factors, etc., are difficult to capture with the classical approaches to availability analysis.

## 9.2 Modeling solutions

The typical engineer can perform back-of-the-envelope analyses easily. Results from these analyses are only as good as the assumed ground rules and the data used. Experience has shown that analysts who wish to perform availability studies often and consistently should choose a software package to aid in this effort. Packages exist that perform analyses via most of the described methodologies. Once a package is selected, the user should become familiar with the package behavior, the analytical or numerical methodology used, and the underlying limitations of that package.

## 10. Common cause failures (CCF)

Dependent failures are those events that inadvertently affect the redundancy or diversity that is employed to improve the availability of a system. In the absence of dependent failures, separate sets of a redundant system, or diverse methods of providing the same function, are regarded as independent. The unavailability of the function is essentially the product of the unavailabilities of the separate trains or diverse systems. However, a dependent failure arises from some cause that fails more than one system, or more than one

train of a system, simultaneously. Thus, the effect of dependent failures is to increase the unavailability of the system function compared to cases where failures are independent. In terms of system reliability modeling, incorporation of the effects of dependent failures into the model provides more realistic estimates of system unavailability [B10], [B17].

It is important to distinguish between common cause failures and common mode failures. Common mode failures refer to coincident failures of the same mode in two different systems or components. For example, two turbine generators may fail due to a crack in their shafts. On the other hand, common cause failures are those events that have the same underlying cause. For example, excessive environmental pollution and humidity may cause flashover on bushings of a power transformer and its redundant unit at the same time.

Considering the importance of software in proper and reliable operation of systems and the fact that failures in software-based systems are not well understood, special care should be taken when modeling systems that contain software-based components.

## 10.1 Common cause failure analysis procedure

U.S. Nuclear Regulatory Commission (NRC) organizes the CCF failure analysis in three phases [B10]:

Phase I: Screening analysis

Phase II: Detailed qualitative analysis

Phase III: Detailed quantitative analysis

The main objectives of the screening analysis include identifying all the potential vulnerabilities of the system to CCFs and identifying the set of components within the system whose CCFs contribute significantly to the system unavailability.

Phase II aims at developing an understanding of the plant-specific vulnerabilities to CCFs by evaluating the susceptibility of the systems and components at a specific plant to causes and coupling factors of CCFs found throughout the industry. This involves the identification of plant-specific defenses in place and qualitative evaluation of their effectiveness. The results of the qualitative analysis form the basis to improve the defenses against CCFs and reduce the likelihood of their occurrence.

Detailed quantitative analysis in Phase III includes common cause modeling, data analysis and parameter estimation, and system quantification and results interpretation.

Detail study of common cause failure is outside the scope of this recommended practice, however it is strongly recommended not to lose sight of common cause failures through questionable assumptions while studying system availability. A recent example of major catastrophe set off by common cause failure is the Fukushima disaster in Japan in early 2011. A single event led to the loss of off-site electrical power to the reactor complex, the loss of oil tanks and replacement fuel for diesel generators, the flooding of the electrical switchyard, and perhaps damage to the inlets bringing in cooling water from the ocean. In other words, one event (tsunami) caused the main system and its backup(s) to fail.

Further details and additional examples of CCF can be found in many books and white papers including “Incorporating Common Cause Failures in Mission Critical Facilities Reliability Analysis” [B11] published in *IEEE Transactions on Industry Application* in 2014.

## Annex A

(informative)

## Bibliography

Bibliographical references are resources that provide additional or helpful material but do not need to be understood or used to implement this standard. Reference to these resources is made for informational use only.

[B1] Anthony, M., R. Arno, N. Dowling, and R. Schuerger, “Reliability Analysis for Power to Fire Pump Using Fault Tree and RBD,” IEEE/IAS Industrial & Commercial Power Systems Technical Conference (I&CPS), Louisville, KY, 2012.

[B2] Billinton, R. and R. N. Allan, *Reliability Evaluation of Engineering Systems, Concepts and Techniques*, 2nd ed. New York, NY: Plenum Press, 1992.

[B3] Billinton, R. and R. N. Allan, *Reliability Evaluation of Power Systems*, 2nd ed. New York, NY: Plenum Press, 1996.

[B4] Department of the Army TM 5-698-1, Reliability/Availability Analysis of Electrical and Mechanical Systems for Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) Facilities, 14 March 2003.

[B5] Department of the Army TM 5-698-3, Reliability Primer for Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) Facilities, 10 July 2003.

[B6] Ebeling, C. E., *An Introduction to Reliability and Maintainability Engineering*, Waveland Press, Long Grove, IL, 2005.

[B7] MIL-STD-339 (1998), Selection and Installation of Wiring and Wiring Devices for Combat and Tactical Vehicles.

[B8] Kumamoto, H. and E. J. Henley, *Probabilistic Risk Assessment and Management for Engineers and Scientists*, 2nd ed., IEEE Press, Piscataway, NJ, 1996.

[B9] Meeker, W. Q. and L. A. Escobar, *Statistical Methods for Reliability Data*, Wiley-Interscience, 1998.

[B10] Mosleh, A., D. M. Rasmuson, and F. M. Marshall, “Guidelines on Modeling Common Cause Failures in Probabilistic Risk Assessments,” Safety Programs Division, Office for Analysis and Evaluation of Operational Data, U.S. Nuclear Regulatory Commission, Washington, D.C. 20555, NUREG/CR-5485, INEEL/EXT-97-01327, 1997.

[B11] Pourali, M., “Incorporating Common Cause Failures in Mission Critical Facilities Reliability Analysis,” *IEEE Transactions on Industry Applications*, July/August 2014, Vol. 50, Issue 4, pp. 1-8.

[B12] Pourali, M., “The Supremacy of Embedded Redundancy over Redundancy at System Level in Mission Critical Facilities,” IEEE Industry Applications Society Annual Meeting, 2009.

[B13] *Reliability Growth and Repairable System Data Analysis Reference*, ReliaSoft Publishing, 2009.

[B14] Reliability Analysis Center, “Practical Statistical Tools for the Reliability Engineer,” 1999.

[B15] Reliability Analysis Center, “Reliability Toolkit: Commercial Practices Edition,” 1994.

[B16] Rausand, M. and A. Hoyland, *System Reliability Theory, Models, Statistical Methods, and Applications*, John Wiley & Sons, Hoboken, NJ, 2004.

[B17] Smith, D. J., *Reliability, Maintainability and Risk, Practical Methods for Engineers*, 7th ed., Elsevier Butterworth-Heinemann, Burlington, MA, 2005.





# Consensus

WE BUILD IT.

**Connect with us on:**



**Facebook:** <https://www.facebook.com/ieeesa>



**Twitter:** @ieeesa



**LinkedIn:** <http://www.linkedin.com/groups/IEEESA-Official-IEEE-Standards-Association-1791118>



**IEEE-SA Standards Insight blog:** <http://standardsinsight.com>



**YouTube:** IEEE-SA Channel

---

IEEE

[standards.ieee.org](http://standards.ieee.org)

Phone: +1 732 981 0060 Fax: +1 732 562 1571

© IEEE